(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－99462
（P2000－99462A）
(43)公開日　平成12年４月７日(2000.4.7)

| (51)Int.Cl.⁷ | 識別記号 | ＦＩ | | テーマコード（参考） |
|---|---|---|---|---|
| Ｇ０６Ｆ　15/00 | ３１０ | Ｃ０６Ｆ　15/00 | ３１０Ｅ | |
| 13/00 | ３５１ | 13/00 | ３５１Ｚ | |
| Ｈ０４Ｌ　9/32 | | Ｈ０４Ｌ　9/00 | ６７５Ａ | |

審査請求　未請求　請求項の数15　ＯＬ　（全 10 頁）

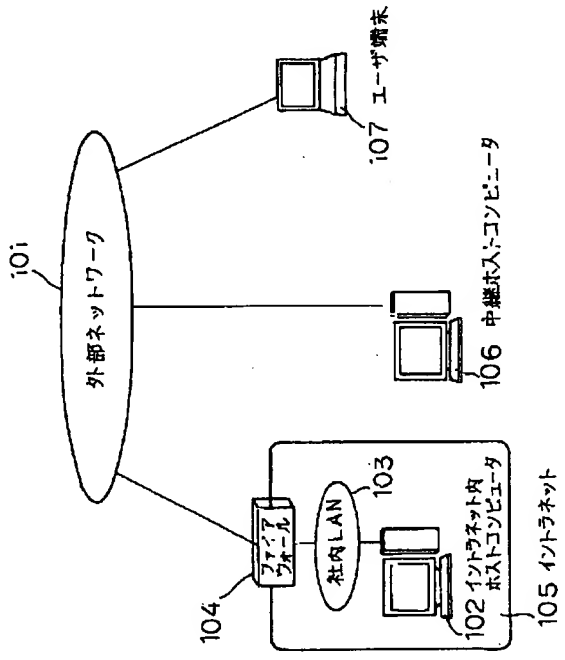
(21)出願番号　特願平10－271650

(22)出願日　平成10年９月25日(1998.9.25)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　堀岡　力
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　曽根原　登
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(72)発明者　竹下　敦
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　100070219
弁理士　若林　忠　（外２名）

(54)【発明の名称】　遠隔操作方法、システム、および遠隔操作プログラムを記録した記録媒体

(57)【要約】
【課題】　イントラネットに直接接続することなくイントラネット内のホストコンピュータに対して安全に操作を実行する。
【解決手段】　イントラネット内ホストコンピュータ２２０との認証情報を作成する。次に、操作情報を作成し、作成した操作情報を暗号化する。暗号化された操作情報と認証情報を中継ホストコンピュータ１０６に送信する。中継ホストコンピュータ１０６では、認証情報と暗号化操作情報を受取り、ホストコンピュータ１０２が受信可能なデータ形式に変換し、データ変換された認証情報と暗号化操作情報をホストコンピュータ１０２へ送信する。ホストコンピュータ１０２では、認証情報と暗号化された操作情報を受信し、ユーザ認証を行う。ユーザの正当性が証明されると、蓄積されている暗号化操作情報を復号するための鍵を取得し、暗号化操作情報を復号する。復号された操作情報の実行権が確認され、実行される。



【特許請求の範囲】

【請求項1】 遠隔地から安全性が保証されていない外部ネットワークを介して、イントラネット内のホストコンピュータまたは該ホストコンピュータに接続されたコンピュータに対して操作を行う遠隔操作方法であって、遠隔地の外部ネットワークに接続された端末上で操作方法を作成し、前記操作方法を暗号化し、前記暗号化された操作方法を前記外部ネットワーク上に設置された中継ホストコンピュータへ送信し、前記中継ホストコンピュータから前記イントラネット内のホストコンピュータへ前記暗号化操作方法を送信し、前記イントラネット内のホストコンピュータで前記暗号化された操作方法を復号し、前記操作を操作対象コンピュータに対して実行する遠隔操作方法。

【請求項2】 前記イントラネット内の操作対象コンピュータに対して操作を実行する際に必要な情報を予め暗号化し、前記外部ネットワーク上の中継ホストコンピュータに前記暗号化情報を蓄積し、前記ユーザが前記端末からイントラネット内の操作対象コンピュータに対して操作を実行する際に、前記中継ホストコンピュータに蓄積された暗号化情報を取得し、前記暗号化情報を復号し、前記復号された情報を用いて前記操作方法を作成する請求項1記載の遠隔操作方法。

【請求項3】 操作方法を作成する際に、ユーザの正当性を証明するためのユーザ認証情報を作成し、前記暗号化された操作方法と一緒に前記中継ホストコンピュータへ送信し、前記中継ホストコンピュータで前記受信した暗号化操作方法とユーザ認証情報を前記イントラネット内のホストコンピュータへ送信し、前記イントラネット内のホストコンピュータで前記ユーザ認証情報を基にユーザの正当性を証明した後に、前記暗号化操作方法を復号し、前記操作を実行する請求項1または2記載の遠隔操作方法。

【請求項4】 前記中継ホストコンピュータに蓄積された暗号化情報を取得する際に、該中継ホストコンピュータがユーザの正当性を証明した後、暗号化情報を取得する、請求項2または3記載の遠隔操作方法。

【請求項5】 遠隔地から安全性が保証されていない外部ネットワークを介して、イントラネット内のホストコンピュータまたは該ホストコンピュータに接続されたコンピュータに対して操作を行う遠隔操作方法であって、遠隔地の外部ネットワークに接続された端末上で操作方法を作成する操作情報作成手段と、前記操作方法を暗号化する暗号化手段と、外部ネットワーク上の中継ホストコンピュータへ前記暗号化された操作方法を送信する送信手段と、前記外部ネットワーク上の中継ホストコンピュータで、前記端末から送信された暗号化された操作方法を受信する受信手段と、イントラネット内のホストコンピュータで、前記中継ホストコンピュータを介して前記端末から送信された前記暗号化された操作方法を受信する受信手段と、前記暗号化された操作方法を復号する復号手段と、前記復号された操作方法を操作対象コンピュータに対して実行する操作実行手段を有する遠隔操作システム。

【請求項6】 前記イントラネット内の操作対象コンピュータに対して操作を実行する際に必要な情報を暗号化する暗号化手段と、前記暗号化された情報を前記中継ホストコンピュータへ送信する暗号化情報送信手段と、中継ホストコンピュータで前記暗号化された情報を蓄積する蓄積手段と、前記端末からの要請により前記暗号化された情報を前記端末へ送信する暗号化情報送信手段をさらに有する請求項5記載の遠隔操作システム。

【請求項7】 操作方法を作成する際に前記端末上でユーザの正当性を証明するユーザ認証情報を作成する手段と、イントラネット内ホストコンピュータで前記ユーザ認証情報を基にユーザの正当性を証明する手段をさらに有する請求項5または6記載の遠隔操作システム。

【請求項8】 前記中継ホストコンピュータから暗号化された情報を取得する際に、ユーザの正当性を証明するユーザ認証情報を前記端末上で作成する手段と、前記中継ホストコンピュータ上で前記ユーザ認証情報を基にユーザの正当性を証明する手段をさらに有する請求項6または7記載の遠隔操作システム。

【請求項9】 遠隔地の外部ネットワークに、イントラネット内のホストコンピュータまたは該ホストコンピュータに接続されたコンピュータに対して行う操作方法を作成する手順と、作成された前記操作方法を暗号化する手順と、前記暗号化された操作方法を、前記外部ネットワークに設置された中継ホストコンピュータへ送信する手順をコンピュータに実行させるための端末側遠隔操作プログラムを記録した記録媒体。

【請求項10】 請求項9記載の前記中継ホストコンピュータから前記イントラネット内のホストコンピュータへ送信された前記暗号化された操作方法を復号する手順と、復号された操作方法を実行する手順をコンピュータに実行させるためのホストコンピュータ側遠隔操作プログラムを記録した記録媒体。

【請求項11】 ユーザがイントラネット内のホストコンピュータまたは該ホストコンピュータに接続されたコンピュータで操作を実行する際に必要な情報を予め暗号化する手順と、前記暗号化された情報を中継ホストコンピュータに送信する手順と、前記中継ホストコンピュータから前記暗号化された情報を取得し、復号する手順と、復号された情報を用いて、前記イントラネット内の操作対象コンピュータに対して行う操作方法を作成する手順と、前記操作方法を暗号化する手順と、前記暗号化された操作方法を前記中継コンピュータへ送信する手順をコンピュータに実行させるための端末側遠隔操作プログラムを記録した記録媒体。

【請求項12】 請求項11記載の暗号化された情報を

蓄積する手順と、蓄積されている、暗号化された情報を前記端末側へ送信する手順をコンピュータに実行させるための中継ホストコンピュータ側遠隔操作プログラムを記録した記録媒体。

【請求項13】 操作方法を作成する際に、ユーザの正当性を証明するためのユーザ認証情報を作成する手順と、前記ユーザ認証情報を前記暗号化された操作方法とともに前記中継ホストコンピュータに送信する手順をさらに有する、請求項9記載の記録媒体。

【請求項14】 前記中継ホストコンピュータから前記ホストコンピュータへ前記暗号化操作方法とともに送信されたユーザ認証情報を基にユーザ認証を行う手順をさらに有する、請求項10記載の記録媒体。

【請求項15】 前記中継ホストコンピュータ上で、ユーザが前記中継ホストコンピュータから暗号化された情報を取得する際に作成した、ユーザの正当性を証明するユーザ認証情報を基にユーザ認証を行う手順をさらに有する、請求項12記載の記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、遠隔地から安全性が保証されていない外部ネットワークを介して、インントラネット内のホストコンピュータまたは該ホストコンピュータに接続されたコンピュータに対して操作を実行する遠隔操作方法、システム、および遠隔操作プログラムを記録した記録媒体に関する。

【0002】

【従来の技術】ネットワークの発達により、遠隔地から、イントラネット内のホストコンピュータまたはホストコンピュータに接続されているコンピュータに対して操作を実行させたいという要求が高まっている。

【0003】

【発明が解決しようとする課題】遠隔地からインターネット等の外部ネットワークを介してイントラネット内のホストコンピュータまたはホストコンピュータに接続されているコンピュータに対して操作を実行する場合、ユーザは、イントラネットに直接接続する必要があった。

【0004】インターネット等の安価であるが安全性が保証されていないネットワークを外部ネットワークとして利用する場合、安全性を保証するために通信プロトコル上で暗号通信を行うため、端末や利用環境が限定されるという問題があった。

【0005】本発明の目的は、イントラネット内ホストコンピュータ等への安全な操作の実行と、イントラネット等の安全性が保証されていないネットワークを介してイントラネット内のホストコンピュータ等での操作の実行と、既存の通信プロトコルおよび端末を利用した環境で安全にイントラネット内ホストコンピュータ等への操作を実行する遠隔操作方法、システム、および遠隔操作プログラムを記録した記録媒体を提供することにある。

【0006】

【課題を解決するための手段】本発明の遠隔操作方法は、遠隔地の外部ネットワークに接続された端末上で操作方法を作成し、前記操作方法を暗号化し、前記暗号化された操作方法を前記外部ネットワーク上に設置された中継ホストコンピュータへ送信し、前記中継ホストコンピュータから前記イントラネット内のホストコンピュータへ前記暗号化操作方法を送信し、前記イントラネット内のホストコンピュータで前記暗号化された操作方法を復号し、前記操作を操作対象コンピュータに対して実行する。

【0007】また、本発明の遠隔操作システムは、遠隔地の外部ネットワークに接続された端末上で、操作方法を作成する操作情報作成手段と、前記操作方法を暗号化する暗号化手段と、外部ネットワーク上の中継ホストコンピュータへ前記暗号化された操作方法を送信する送信手段と、前記外部ネットワーク上の中継ホストコンピュータで、前記端末から送信された暗号化された操作方法を受信する受信手段と、イントラネット内のホストコンピュータで、前記中継ホストコンピュータを介して前記端末から送信された前記暗号化された操作方法を受信する手段と、前記暗号化された操作方法を復号する復号手段と、前記復号された操作方法を操作対象コンピュータに対して実行する操作実行手段を有する。

【0008】本発明は、ユーザが遠隔地から外部ネットを介してイントラネット内のホストコンピュータまたはホストコンピュータに接続されたコンピュータに対して操作を実行する場合、イントラネットに直接接続することなく、外部ネットワーク上に設置された中継ホストコンピュータに操作を依頼することにより、イントラネット内のホストコンピュータまたはホストコンピュータに接続されたコンピュータに対する操作を実行する。

【0009】中継ホストコンピュータとユーザ端末間の通信、および中継ホストコンピュータとイントラネット内ホストコンピュータとの間の通信は、既存の通信プロトコルと端末を用いて実現可能である。

【0010】本発明の実施態様によれば、イントラネット内の操作対象コンピュータに対して操作を実行する際に必要な情報を予め暗号化し、前記外部ネットワーク上の中継ホストコンピュータに前記暗号化情報を蓄積し、前記ユーザが端末からイントラネット内の操作対象コンピュータに対して操作を実行する際に、前記中継ホストコンピュータに蓄積された暗号化情報を取得し、前記暗号化情報を復号し、前記復号された情報を用いて前記操作方法を作成する。

【0011】本発明の実施態様によれば、操作方法を作成する際に、ユーザの正当性を証明するためのユーザ認証情報を作成し、前記暗号化された操作方法と一緒に前記中継ホストコンピュータへ送信し、前記中継ホストコンピュータで前記受信した暗号化操作方法とユーザ認証

情報を前記イントラネット内のホストコンピュータへ送信し、前記イントラネット内のホストコンピュータで前記ユーザ認証情報を基にユーザの正当性を証明した後に、前記暗号化操作方法を復号し、前記操作を実行する。

【００１２】本発明の他の実施態様によれば、前記中継ホストコンピュータに蓄積された暗号化情報を取得する際に、該中継ホストコンピュータがユーザの正当性を証明した後、暗号化情報を取得する。

【００１３】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して説明する。

【００１４】（第１の実施の形態）本発明の第１の実施形態として、イントラネット内のホストコンピュータに対して、外部ネットワークに接続された遠隔地のユーザ端末からユーザが操作を行う例を説明する。

【００１５】図１は本実施形態のシステムの概略構成図である。

【００１６】イントラネット１０５と中継ホストコンピュータ１０６とユーザ端末１０７が、インターネット等のような安全性が保証されていない外部ネットワーク１０１を介して互いに接続されている。イントラネット１０５は、イントラネット内ホストコンピュータ１０２と社内ＬＡＮ１０３とファイアウォール１０４からなる。

【００１７】イントラネット１０５内のホストコンピュータ１０２は社内ＬＡＮ１０３に接続されており、外部ネットワーク１０１とは、社内ＬＡＮ１０３とファイアウォール１０４を介してデータの送受信が可能である。ファイアウォール１０４は設定により不法な接続を拒絶する。中継ホストコンピュータ１０６は、予め設定されたプロトコルでの接続のみ許可している。ユーザ端末１０７は、外部ネットワーク１０１に直接接続していても、イントラネット１０５と異なるイントラネット内の社内ＬＡＮ１０３に接続されていても問題ない。

【００１８】図２は図１中のユーザ端末１０７、中継ホストコンピュータ１０６、イントラネット内ホストコンピュータ１０２の概略構成図である。

【００１９】ユーザ端末１０７はデータ入力部２０１と認証情報作成部２０２と操作情報作成部２０３とデータ暗号化部２０４とデータ送信部２０５を有している。

【００２０】中継ホストコンピュータ１０６はデータ受信部２１１とデータ形式変換部２１２とデータ送信部２１３を有している。

【００２１】イントラネット内ホストコンピュータ１０２はデータ受信部２２１とユーザ認証部２２２と認証情報蓄積部２２３と復号鍵取得部２２４と復号鍵蓄積部２２５とデータ復号部２２６と操作実行権確認部２２７と操作実行部２２８からなる。

【００２２】ユーザが外部ネットワーク１０１に接続されたユーザ端末１０７からイントラネット内ホストコンピュータ１０２に対して操作を実行する場合、まず認証情報作成部２０２において、データ入力部２０１から入力された秘密のパスワードを基に、イントラネット内ホストコンピュータ１０２との認証情報を作成する。次に、イントラネット内ホストコンピュータ１０２上で実行する操作の操作情報を、データ入力部２０１から入力されたデータを基に操作情報作成部２０３において作成し、データ暗号化部２０４において作成した操作情報を暗号化する。暗号化された操作情報と認証情報をデータ送信部２０５により中継ホストコンピュータ１０６に送信する。

【００２３】中継ホストコンピュータ１０６では、認証情報と暗号化操作情報をデータ受信部２１１で受取り、データ形式変換部２１２でイントラネット内ホストコンピュータ１０２が受信可能なデータ形式に変換する。データ変換された認証情報と暗号化操作情報はデータ送信部２１３でイントラネット内ホストコンピュータ１０２へ送信する。

【００２４】イントラネット内ホストコンピュータ１０２では、データ受信部２２１で認証方法と暗号化された操作情報を受信し、認証情報蓄積部２２３からの情報と受信した認証情報を基に、ユーザ認証部２２２においてユーザ認証を行う。ユーザの正当性が証明されると、復号鍵蓄積部２２５に蓄積されている、暗号化操作情報を復号するための鍵を復号鍵取得部２２４において取得する。取得した鍵を用いてデータ復号部２２６において暗号化操作情報を復号する。復号された操作情報の実行権が操作実行権確認部２２７において確認され、実行権を有している場合のみ、操作実行部２２８において操作を実行する。

【００２５】図３に本実施形態の処理をフローチャートで記す。

【００２６】認証データを作成し（ステップ３０１）、イントラネット内ホストコンピュータ１０２の操作を行うための操作情報を作成する（ステップ３０２）。操作情報を暗号化し（ステップ３０３）、中継ホストコンピュータ１０６へ送信する。中継ホストコンピュータ１０６では、データ形式の変換を行い、イントラネット内ホストコンピュータ１０２へ認証情報と暗号化された操作情報を送信する（ステップ３０４）。送信後、正しく送信が行われたことを確認し、ユーザ端末１０７へ通知する（ステップ３０５）。イントラネット内ホストコンピュータ１０２は、受信した認証情報を基にユーザ認証を行い（ステップ３０６）、暗号化された操作情報を復号する（ステップ３０７）。復号された操作情報の実行権を確認し（ステップ３０８）、操作実行権を有する場合、操作を実行する（ステップ３０９）。

【００２７】（第２の実施の形態）次に、本発明の第２の実施形態として、遠隔地のユーザがインターネットに接続されたユーザ端末からイントラネット内のホストに

対し決済処理を行う例について説明する。

【0028】本実施形態の全体のシステム構成は図4に示す通りである。イントラネット405と中継ホストコンピュータ406とイントラネット410がインターネット401を介して互いに接続されている。イントラネット405は、社内LAN403と、社内LAN403に接続されたイントラネット内ホストコンピュータ402と、ファイアウォール404からなる。イントラネット410は、社内LAN408と、社内LAN408に接続されたユーザ端末407と、ファイアウォール409からなる。

【0029】ユーザは、イントラネット410内の社内LAN408に接続されたユーザ端末407からインターネット401を介して、イントラネット405内のイントラネット内ホストコンピュータ402に対し決済処理を実行する。

【0030】ユーザ端末407は、インターネット401上の中継ホストコンピュータ406と通信することが可能であり、ファイアウォール409に設定されたプロトコルで通信を行う。

【0031】イントラネット内ホストコンピュータ402は、インターネット401上の中継ホストコンピュータ406と、ファイアウォール404に設定されたプロトコルを用いて通信を行う。

【0032】本実施形態では、ユーザ端末407と中継ホストコンピュータ406間の通信速度に比べ、イントラネット内ホストコンピュータ402と中継ホストコンピュータ406の通信速度が遅いか、ユーザ端末407とイントラネット内ホストコンピュータ402がファイアウォール404または409により直接通信が行えない場合を想定している。

【0033】イントラネット内ホストコンピュータ402と中継ホストコンピュータ406間の通信プロトコルと、ユーザ端末407と中継ホストコンピュータ406間の通信プロトコルは、例えばHTTP（Hypter Text Transfer Protocol)とSMTP(Simple Mail Transfer Protocol）等のように、異なっていてもよい。

【0034】本実施形態においては、決済に必要なデータが中継ホストコンピュータ406に蓄積されており、中継ホストコンピュータ406とのユーザ認証後に取得できるものとする。

【0035】図5はユーザ端末407の構成を示している。ユーザ端末407は認証作成部504において中継ホストコンピュータ406との認証を行うための認証データを、データ入力部502からユーザ501が入力したデータを基に作成し、作成した認証データをデータ送信部508を介して中継ホストコンピュータ406へ送信する。中継ホストコンピュータ406は、ユーザ認証を行い、ユーザの正当性が証明されると、蓄積されている暗号化決済リストを取得し、ユーザ端末407へ送信する。ユーザ端末407は、データ受信部509において暗号化決済リストを取得する。ユーザ501はデータ入力部502より復号鍵を入力し、暗号化データ復号部507において、暗号化決済リストを復号し、データ表示部503に表示する。

【0036】データ表示部503に表示されている決済リスト512を基に、ユーザ501はデータ入力部502からデータを入力し、操作データ作成部505において、決済データ510を作成する。

【0037】データ暗号化部506において、作成された決済データ510を暗号化し、暗号化決済データ511を作成する。認証情報作成部504において、イントラネット内ホストコンピュータ402との認証に必要な認証データを作成する。データ送信部508により、作成された暗号化決済データと認証データを中継ホストコンピュータ406へ送信する。

【0038】図6は中継ホストコンピュータ406の構成を示している。ユーザ501から暗号化決済リストの要求があった場合、データ受信部601で受信した認証データを基にユーザ認証部604でユーザ認証を行い、ユーザの正当性を証明されると、暗号化データ蓄積部606より、ユーザから指定されたデータである暗号化決済リスト607を暗号化データ取得部605で取得し、取得した暗号化決済リスト607をデータ送信部603でユーザ端末407へ送信する。中継ホストコンピュータ406は、蓄積されているデータが決済リストかどうかを判別しない。そのため、ユーザ認証後に、ユーザごとに蓄積されているデータの蓄積リストを送信し、ユーザが蓄積リスト内から必要なデータを取得することが可能であることは言うまでもない。

【0039】また、ユーザからイントラネット内ホストコンピュータ402へデータを送信する依頼を受信した場合、中継ホストコンピュータ406は、データ受信部601において受信したデータをイントラネット内ホストコンピュータ402へ送信するために、データ形式変換部602でデータ形成の変換を行う。変換されたデータをイントラネット内ホストコンピュータ402へ送信し、正しく送信処理を行ったことをユーザへ通知する。

【0040】図7はイントラネット内ホストコンピュータ402の構成を示している。データ受信部701において、受信した認証データと暗号化決済データのうち、認証データを基にユーザ認証部702においてユーザ認証を行う。ユーザの正当性が証明されると、復号鍵取得部716において復号鍵蓄積部715より取得した復号鍵を用いて、受信した暗号化決済データを操作データ復号部703において復号し、決済データ713を取得する。

【0041】操作実行権確認部704において、該ユーザが、指定した操作である決済の実行権を有しているかどうか確認を行い、実行権を有していると判断された場

合は、決済データ７１３に従い、操作実行部７０５で決済の処理を行う。

【００４２】また、ユーザの指定により、決済リスト蓄積部７１０に蓄積されている決済リスト７１３を予め登録されている暗号化鍵を用いて、決済リスト暗号化部７１１において暗号化し、暗号化決済リスト７１４を作成する。作成された暗号化決済リスト７１４をデータ送信部７１２より、インターネット４０１上の中継ホストコンピュータ４０６へ送信する。

【００４３】表１は決済リストを示しており、本実施形態では、ユーザは決済番号３５の決済依頼に対する決済処理を行う。

【００４４】

【表１】

| No. | タイトル | 内容 |
|---|---|---|
| 1 | 年休の申請 | 98．08．10～98．08．20 |
| 2 | 固定資産の購入 | パソコン一式 |
| ： | ： | ： |
| 35 | 旅費申請 | 北海道出張 |
| ： | ： | ： |

図８に決済データの例を示しており、操作として決済処理が行われ、リスト番号３５の旅費申請に対する決済処理を実行させることを示している。また、ユーザ端末４０７において決済データを簡易に作成するためのフォーマットを予め暗号化し、中継ホストコンピュータ４０６に蓄積しておき、中継ホストコンピュータ４０６で正当性が証明された場合に、暗号化された決済データとともに取得することも可能であることは言うまでもない。

【００４５】図９は、決済実行までの全体の処理フローを示している。

【００４６】ユーザ端末４０７において認証データを作成し（ステップ８０１）、作成された認証データを中継ホストコンピュータ４０６へ送信する（ステップ８０２）。

【００４７】中継ホストコンピュータ４０６は、ユーザ認証を行い（ステップ８０３）、ユーザの正当性が証明されると暗号化データの取得を行う（ステップ８０４）。取得した暗号化データをユーザ端末４０７へ送信する（ステップ８０５）。

【００４８】ユーザ端末４０７は取得した暗号化データを復号し、決済リストを取得する（ステップ８０６）。取得した決済リストを基に決済データを作成し（ステップ８０７）、作成した決済データを暗号化する（ステップ８０８）。イントラネット内ホストコンピュータ４０２と認証を行うための認証データを作成し（ステップ８０９）、暗号化決済データと認証データを中継ホストコンピュータ４０６へ送信する（ステップ８１０）。

【００４９】中継ホストコンピュータ４０６は、受信した暗号化決済リストと認証データのデータ形式の変換を行い（ステップ８１１）、イントラネット内ホストコンピュータ４０２が受信可能な通信プロトコルを用いて送信する（ステップ８１２）。送信後、正しく送信処理を行ったことをユーザ端末４０７へ通知する（ステップ８１３）。

【００５０】イントラネット内ホストコンピュータ４０２は、受信した認証データを基にユーザ認証を行い（ステップ８１４）、ユーザの正当性が証明されると、暗号化決済データを予め登録してある復号鍵を用いて復号し（ステップ８１５）、指定されている操作である決済処理の実行権をユーザが有しているかどうか確認を行い（ステップ８１６）、実行権を有していると判断された場合、決済を実行する（ステップ８１７）。

【００５１】本実施形態において、認証情報がインターネット等の安全性が保証されていないネットワーク上で用いても秘密にしているパスワードを盗取することが不可能な認証方法を用いることは言うまでもない。

【００５２】また、データの暗号化・復号に用いる暗号方式として共通鍵暗号方式を用いても、公開鍵暗号方式を用いてもよく、任意の暗号方式で実行可能であることは言うまでもない。

【００５３】また、ホストコンピュータに接続されたコンピュータに対して操作を実行することもできる。

【００５４】なお、図３および図９に示した処理を遠隔操作プログラムとしてフロッピィ・ディスク、ＣＤ－ＲＯＭ、光磁気ディスク、半導体メモリ等の記録媒体に記録しておき、コンピュータに読取って実行することもできる。

【００５５】

【発明の効果】以上述べたように、本発明によれば、イントラネットに直接接続することなく、イントラネット内のホストコンピュータに対し安全に操作を実行することが可能となる。また、インターネット等の安価であるが安全性が保証されていないネットワーク上で既存の通信プロトコルを利用することも可能となり、端末や利用環境の制限がなくなる。

【図面の簡単な説明】

【図１】本発明の一実施形態のシステム構成図である。

【図２】図１中のユーザ端末１０７、中継ホストコンピ

ュータ106、イントラネット内ホストコンピュータ102の構成図である。

【図3】図1の実施形態における遠隔操作の処理を示すフローチャートである。

【図4】本発明の他の実施形態のシステム構成図である。

【図5】図4中のユーザ端末407の構成図である。

【図6】図4中の中継ホストコンピュータ406の構成図である。

【図7】図4中のイントラネットコンピュータ402の構成図である。

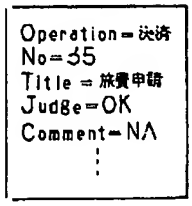
【図8】ユーザがユーザ端末407で作成する決済データの例を示す図である。

【図9】図4の実施形態における決済処理のフローチャートである。

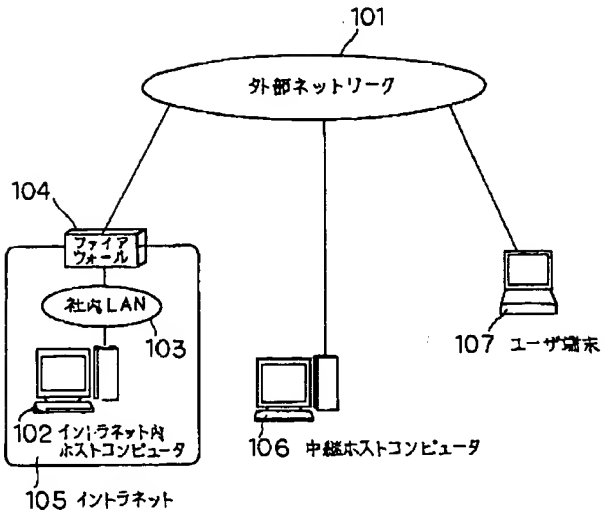
【符号の説明】

101　外部ネットワーク
102　イントラネット内ホストコンピュータ
103　社内LAN
104　ファイアウォール
105　イントラネット
106　中継ホストコンピュータ
107　ユーザ端末
201　データ入力部
202　認証情報作成部
203　操作情報作成部
204　データ暗号化部
205　データ送信部
211　データ受信部
212　データ形成変換部
213　データ送信部
221　データ受信部
222　ユーザ認証部
223　認証情報蓄積部
224　復号鍵取得部
225　復号鍵蓄積部
226　データ復号部
227　操作実行権確認部
228　操作実行部
301～309　ステップ
401　インターネット
402　イントラネット内ホストコンピュータ
403，408　社内LAN
404，409　ファイアウォール
405，410　イントラネット
406　中継ホストコンピュータ
501　ユーザ
502　データ入力部
503　データ表示部
504　認証情報作成部
505　操作データ作成部
506　データ暗号化部
507　暗号化データ復号部
508　データ送信部
509　データ受信部
510　決済データ
511　暗号化決済データ
512　決済リスト
601　データ受信部
602　データ形式変換部
603　データ送信部
604　ユーザ認証部
605　暗号化データ取得部
606　暗号化データ蓄積部
607　暗号化決済リスト
701　データ受信部
702　ユーザ認証部
703　操作データ復号部
704　操作実行権確認部
705　操作実行部
710　決済リスト蓄積部
711　決済リスト暗号化部
712　データ送信部
713　決済リスト
714　暗号化決済リスト
715　復号鍵蓄積部
801～817　ステップ

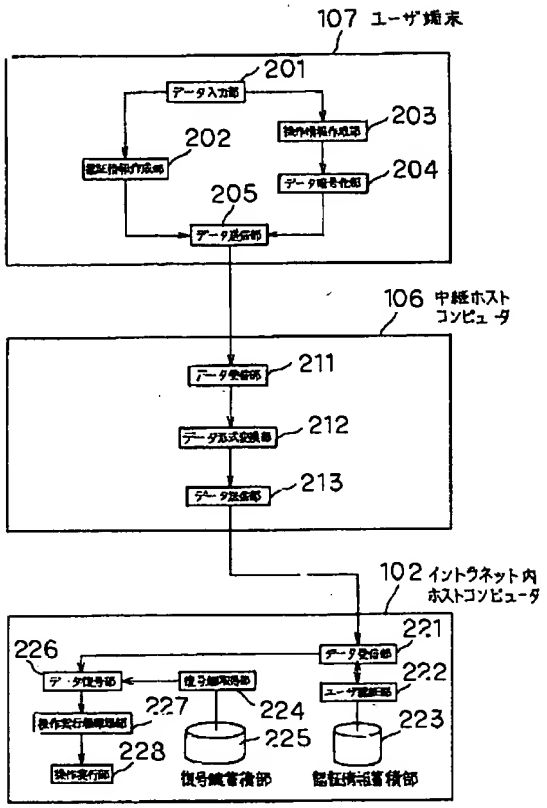
【図8】



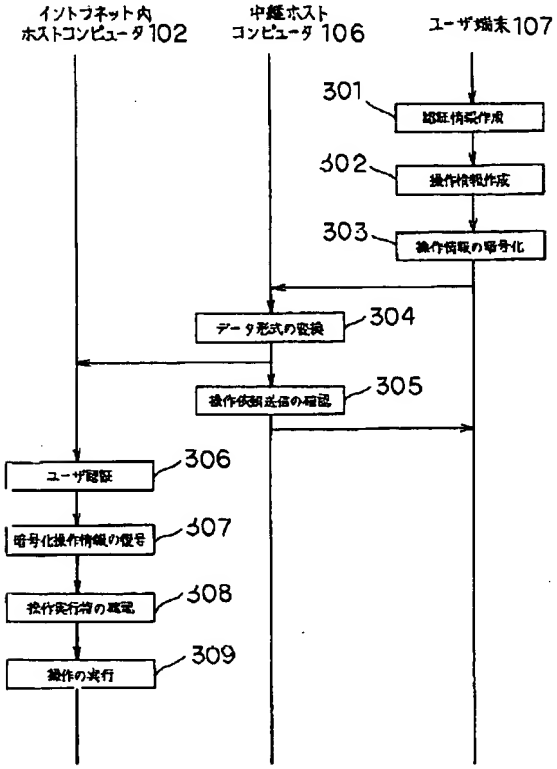
【図1】


101
外部ネットワーク
104
ファイア
ウォール
社内LAN
103
102 イントラネット内
ホストコンピュータ
105 イントラネット
106 中継ホストコンピュータ
107 ユーザ端末

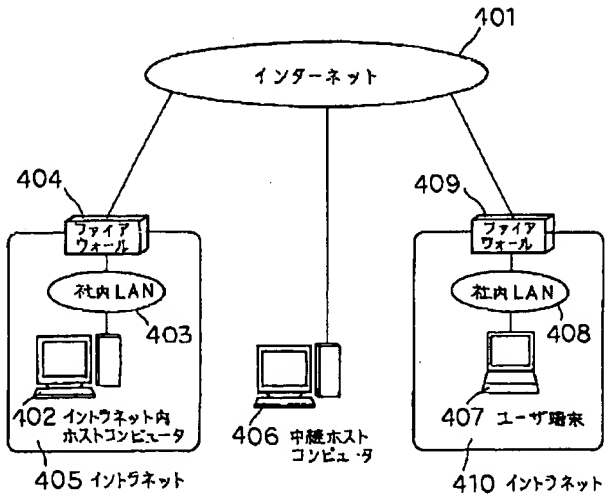
【図2】


107 ユーザ端末
201
データ入力部
202
203
204
205
データ送信部
106 中継ホスト
コンピュータ
211
212
213
102 イントラネット内
ホストコンピュータ
221
222
223
224
225
226
227
228
復号鍵管理部
認証情報蓄積部

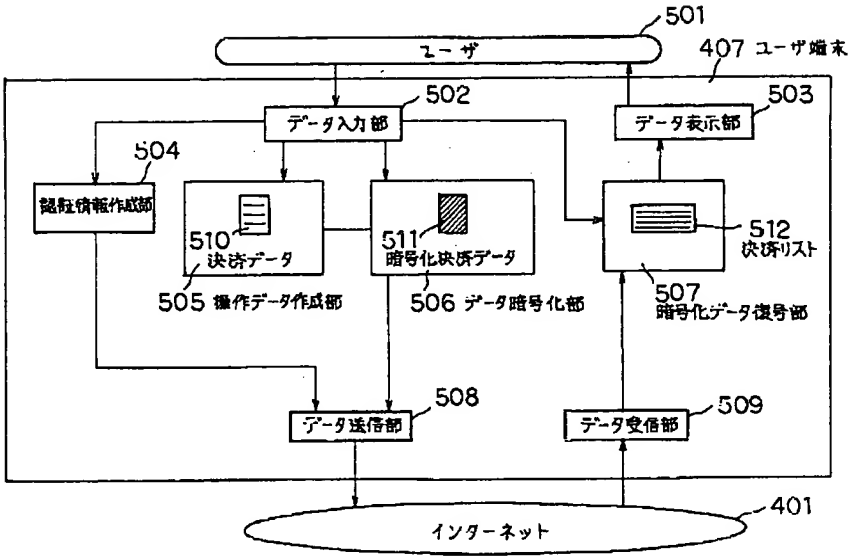
【図3】


イントラネット内
ホストコンピュータ102
中継ホスト
コンピュータ106
ユーザ端末107
301
認証情報作成
302
操作情報作成
303
操作情報の暗号化
304
データ形式の変換
305
306
ユーザ認証
307
暗号化操作情報の復号
308
309
操作の実行

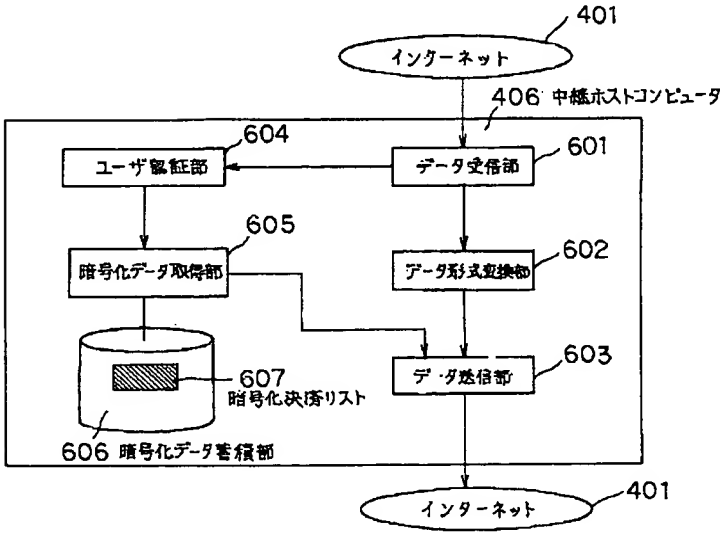
【図4】


401
インターネット
404
ファイア
ウォール
社内LAN
403
402 イントラネット内
ホストコンピュータ
405 イントラネット
406 中継ホスト
コンピュータ
409
ファイア
ウォール
社内LAN
408
407 ユーザ端末
410 イントラネット

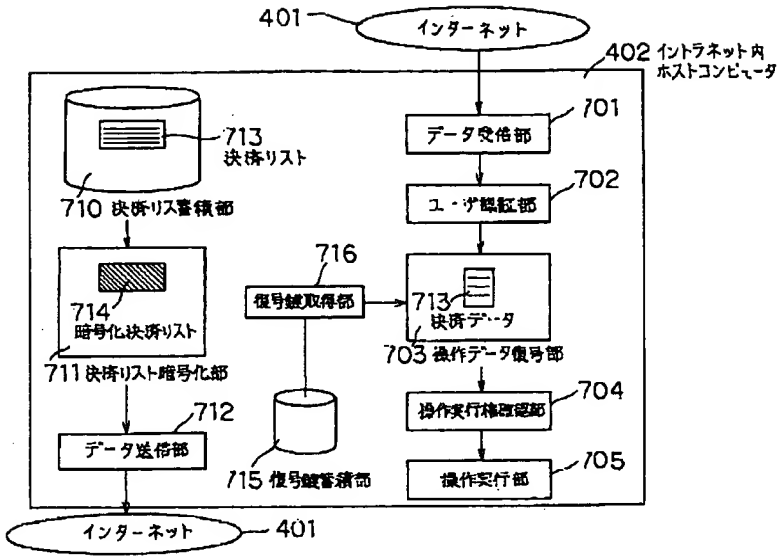
【図5】


501
ユーザ
407 ユーザ端末
502
データ入力部
503
データ表示部
504
認証情報作成部
510
決済データ
511
暗号化決済データ
512
決済リスト
505 操作データ作成部
506 データ暗号化部
507
暗号化データ復号部
508
データ送信部
509
データ受信部
401
インターネット

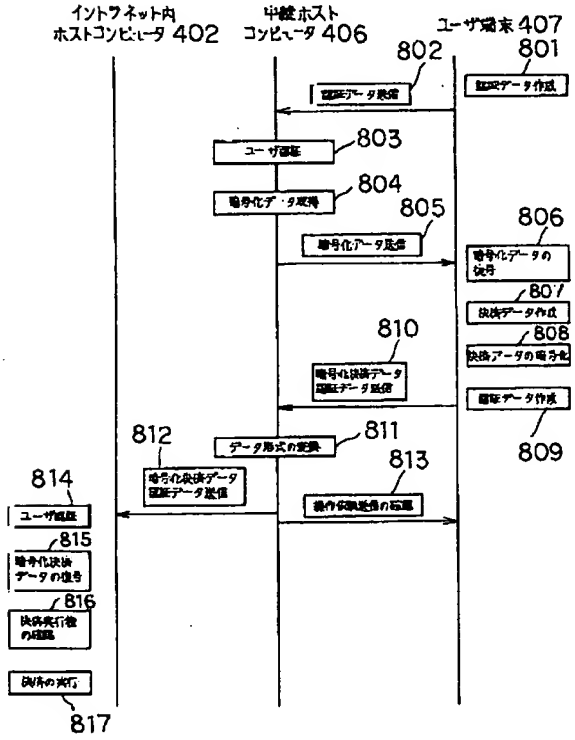
【図6】


401
インターネット
406 中継ホストコンピュータ
604
ユーザ認証部
601
データ受信部
605
暗号化データ取得部
602
データ形式変換部
603
データ送信部
607
暗号化決済リスト
606 暗号化データ蓄積部
401
インターネット

【図7】


401
インターネット
402 イントラネット内
ホストコンピュータ
701
データ受信部
702
ユーザ認証部
703 操作データ復号部
704
操作実行権限確認部
705
操作実行部
712
データ送信部
713
決済リスト
710 決済リス蓄積部
714
暗号化決済リスト
711 決済リスト暗号化部
716
復号鍵取得部
713
決済データ
715 復号鍵蓄積部
インターネット
401

【図9】


イントラネット内
ホストコンピュータ 402
中継ホスト
コンピュータ 406
ユーザ端末 407
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817